Test Results for Disk Imaging Tool:
Tableau TX1 Forensic Imager Version 22.3.0

Federated Testing Suite for Disk Imaging

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology's (NIST) Special Programs Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense's Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, and the DHS' Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Web site (https://www.cftt.nist.gov/).

This document reports the results from testing the disk imaging function of Tableau TX1 Forensic Imager Version 22.3.0 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 5.

Federated Testing is an expansion of the CFTT program to provide forensic investigators and labs with test materials for tool testing and to support shared test reports. The goal of Federated Testing is to help forensic investigators to test the tools they use in their labs and to enable sharing of tool test results. CFTT's Federated Testing Forensic Tool Testing Environment and included test suites can be downloaded from https://www.cftt.nist.gov/federated-testing.html and used to test forensic tools. The results can be optionally shared with CFTT, reviewed by CFTT staff, and then shared with the community.

Test results from this and other tools can be found on DHS's computer forensics web page, https://www.dhs.gov/science-and-technology/nist-cftt-reports.

How to Read This Report

This report is organized into the following sections:

1. Tested Tool Description. The tool name, version, vendor information, and support environment version (e.g., operating system version) are listed.
2. Testing Organization. The name and contact information of the organization that performed the tests are listed.
3. Results Summary. This section identifies any significant anomalies observed in the test runs. This section provides a narrative of key findings identifying where the tool meets expectations and provides a summary of any ways the tool did not meet expectations. The section also provides any observations of interest about the tool or about testing the tool including any observed limitations or organization-imposed restrictions on tool use.
4. Test Environment. Description of hardware and software used in tool testing in sufficient detail to satisfy the testing organization's policy and requirements.
5. Test Result Details by Case. Automatically generated test results that identify anomalies.
6. Appendix: Additional Details. Additional administrative details for each test case such as, who ran the test, when the test was run, computer used, etc.

Federated Testing Test Results for Disk Imaging Tool: Tableau TX1 Forensic Imager Version 22.3.0

Tests were Configured for the Following Write Block Scenarios:

Small (< 138GB) SATA drive with write blocker built-in to imaging device connected to PC by SATA interface

Large (> 138GB) SATA drive with write blocker built-in to imaging device connected to PC by SATA interface

USB drive with write blocker built-in to imaging device connected to PC by USB interface

Tool Description

Tool Name: Tableau TX1 Forensic Imager
Tool Version: 22.3.0

File Name: setup_tableau_firmware_update_22.3.msi
SHA1: 9d49a742fe8aace7584acf000ab10e113718d6be
Full Version Number: 22.3.0.1.5001cc549b

Vendor Contact:

Vendor Name: OpenText

     Address: 275 Frank Tompa Drive, Waterloo, ON, N2L 0A1, Canada

     Phone: 519-888-7111

     Web: https://www.opentext.com

Testing Organization

Organization conducting test:
     US Food and Drug Administration (FDA)
     Office of Criminal Investigations (OCI)
     Digital Forensics Unit (DFU)

Authored by: Special Agent Chad Parks
Contact: chad.parks@fda.hhs.gov
Report date: 10/24/2022

Reviewed by: Special Agent Samuel Koffman
Contact: samuel.koffman@oig.hhs.gov
Reviewed by date: 10/28/2022

This test report was generated using CFTT's Federated Testing Forensic Tool Testing
Environment, see Federated Testing Home Page.

Results Summary

The disk imaging tool met expectations for the various imaging scenarios tested.

Test Environment & Selected Cases

Hardware: Tableau TX1 Forensic Imager
Firmware Version: 22.3.0

Write Blockers Used in Testing

Blocker Model	Firmware Version
write blocker built-in to imaging device	n/a

Selected Test Cases

This table presents a brief description of each test case that was performed.

Test Case Status

Case	Description	Status
FT-DI-01-SATA28	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-01-SATA48	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-01-USB	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed

Case	Description	Status
FT-DI-10	Acquire a drive to an image file without enough space for the image file. Test the ability of the tool to notify the user that the image file is incomplete.	completed
FT-DI-13	Compute the hash value of the acquired data within an image file. Test the ability of the tool to recompute the hash of an existing image file.	completed
FT-DI-14	Compute the hash value of a drive (without creating an image file). Test the ability to read all data accurately and correctly hash the data.	completed

Test Result Details by Case

This section presents test results grouped by function.

FT-DI-01

Test Case Description

Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.

This test can be repeated to test acquisition of multiple drive types. This test tests the ability of the tool to acquire a specific type of drive (the drive type tested is included in the test case name) to an image file using a specific write blocker (applies only to tools that are used with hardware write blockers) and a certain interface connection between the test computer and the write blocker. The write blocker used and the interface connection between the test computer and the write blocker are listed for each test case in the table below. Two tests are required to test ATA or SATA drives, one to test drives smaller than 138GB (ATA28 & SATA28: 28-bit addressing) and one to test larger drives (ATA48 & SATA48: 48-bit addressing).

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-01 cases

Case	Src	Blocker (interface)	Reference Hash vs Tool Hash MD5	Reference Hash vs Tool Hash SHA1
FT-DI-01-SATA28	a1	write blocker built-in to imaging device (SATA)	match	match
FT-DI-01-SATA48	a2	write blocker built-in to imaging device (SATA)	match	match
FT-DI-01-Universal Serial Bus (USB)	a6	write blocker built-in to imaging device (USB)	match	match

Case Summary

Results are as expected.

NOTE: FT-DI-01-SATA28 and FT-DI-01-SATA48 were tested using each SATA/SAS source signal connector (SATA/SAS 1 and SATA/SAS 2) writing to each destination connector (SATA/SAS 1, SATA/SAS 2, and USB). FT-DI-01-USB was also tested writing to each destination connector (SATA/SAS 1, SATA/SAS 2, and USB).

FT-DI-10

Test Case Description

Acquire a drive to an image file without enough space for the image file. Test the ability of the tool to notify the user that the image file is incomplete.

Test Evaluation Criteria

The tool should issue a message indicating not enough space for the image file.

Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-10 cases

Case	Message(s)
FT-DI-10	**Message displayed after selecting destination drive**: "Source will not fit on selected destination(s)"; "This will be a partial duplication"; Selection of "Dismiss" required to continue **Job status message:** "Status: Failed"; "Reason: Destination is full" **Log file messages:** "*** CAUTION: THE OPERATION RECORDED IN THIS LOG DID NOT COMPLETE NORMALLY ***"; "Status: Error/Failed"; "Reason for failure: Destination is full"

Case Summary

Results are as expected.

FT-DI-13

Test Case Description

Compute the hash value of the acquired data within an image file. Test the ability of the tool to recompute the hash of an existing image file.

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-13 cases

Case	Src	Reference Hash vs Tool Hash MD5	Reference Hash vs Tool Hash SHA1
FT-DI-13	a2	match	match

Case Summary

Results are as expected.

FT-DI-14

Test Case Description

Compute the hash value of a drive (without creating an image file). Test the ability to read all data accurately and correctly hash the data.

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-14 cases

Case	Src	Reference Hash vs Tool Hash MD5	Reference Hash vs Tool Hash SHA1
FT-DI-14	a2	match	match

Case Summary

Results are as expected.

Appendix: Additional Details

Test drives and Partitions

The following table presents the state of each source object, drive or partition, including reference hashes and known content.

Both drives and partitions are described in the table. Partitions are indicated in the *Drive* column by the notation **[drive]+[partition number]**. Where **[drive]** is the drive label and **[partition number]** is the partition number. For example, the first partition on drive A3 would be A3+1. The type column records either the drive type, e.g. sata, usb, etc., or the partition type, e.g., ntfs, fat32, etc., depending on whether a drive or a partition is being described.

Test Drives

Drive	Type	Content	Sectors	MD5	SHA1	SHA256	SHA512
a1	sata	known	250069680 (119GiB)	7075F ...	46A41 ...	CFF23 ...	8C445 ...
a2	sata	known	1000215216 (476GiB)*	F3EE2 ...	9ED96 ...	6940D ...	C8147 ...
a6	usb	known	122945536 (58GiB)	AE0BA ...	898DB ...	F04F3 ...	83D08 ...

* Large 48-bit address drive

Test Case Admin Details

For each test run, the test computer, the tester, the source drive, the image file drive, the destination drive, and the date the test was run are listed.

ft-di-01-sata28	CHAD_PARKS	Tableau_Tx1_00 0Ecc5802205D	write blocker built-in to imaging device (SATA)	a1	image-01-SATA28.e01	91_92_93	Tue Oct 11 14:26:26 2022 (UTC-0700) / Tue Oct 11 14:52:22 2022 (UTC-0700)
ft-di-01-sata48	CHAD_PARKS	Tableau_Tx1_00 0Ecc5802205D	write blocker built-in to imaging device (SATA)	a2	image-01-SATA48.e01	91_92_93	Wed Oct 12 13:58:16 2022 (UTC-0700) / Thu Oct 13 13:07:49 2022 (UTC-0700)
ft-di-01-usb	CHAD_PARKS	Tableau_Tx1_00 0Ecc5802205D	write blocker built-in to imaging device (USB)	a6	image-01-USB.e01	91_92_93	Thu Oct 13 13:50:49 2022 (UTC-0700)
ft-di-10	CHAD_PARKS	Tableau_Tx1_00 0Ecc5802205D	N/A	a2	image-10.e01 (incomplete)	96	Wed Oct 19 11:24:48 2022 (UTC-0700)
ft-di-13	CHAD_PARKS	Tableau_Tx1_00 0Ecc5802205D	write blocker built-in to imaging device (SATA)	a2	none	none	Fri Oct 14 15:07:09 2022 (UTC-0700)
ft-di-14	CHAD_PARKS	Tableau_Tx1_00 0Ecc5802205D	N/A	a2	none	none	Fri Oct 14 14:38:59 2022 (UTC-0700)

Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions

cftt-di Version 1.25 created 05/23/18 at 15:58:45
diskwipe.c Linux Version 1.5 Created 03/20/13 at 14:23:34

Tool: @(#) ft-di-prt_test_report.py Version 1.24 created 05/23/18 at 16:08:06
OS: Linux Version 4.13.0-37-generic
Federated Testing Version 5, released 3/12/2020